Міністерство освіти і науки України

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Фізико-технічний інститут

**ЛАБОРАТОРНА РОБОТА №3**

З дисципліни«Криптографія»

«Криптоаналіз афінної біграмної підстановки»

Виконали:

студенти 3 курсу ФТІ

групи ФБ-73  
Шишкин Никита

Витрович Анна

Перевірив:

Чорний О.

Завадська Л.О.

Савчук М.М.

**Мета роботи:**

Набуття навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки; опанування прийомами роботи в модулярній арифметиці.

**Порядок виконання роботи:**

0. Уважно прочитати методичні вказівки до виконання комп’ютерного практикуму.

1. Реалізувати підпрограми із необхідними математичними операціями: обчисленням оберненого елементу за модулем із використанням розширеного алгоритму Евкліда, розв’язуванням лінійних порівнянь. При розв’язуванні порівнянь потрібно коректно обробляти випадок із декількома розв’язками, повертаючи їх усі.

2. За допомогою програми обчислення частот біграм, яка написана в ході виконання комп’ютерного практикуму №1, знайти 5 найчастіших біграм запропонованого шифртексту (за варіантом).

3. Перебрати можливі варіанти співставлення частих біграм мови та частих біграм шифртексту (розглядаючи пари біграм із п’яти найчастіших). Для кожного співставлення знайти можливі кандидати на ключ ) ,( b a шляхом розв’язання системи (1).

4. Для кожного кандидата на ключ дешифрувати шифртекст. Якщо шифртекст не є змістовним текстом російською мовою, відкинути цього кандидата.

5. Повторювати дії 3-4 доти, доки дешифрований текст не буде змістовним.

**Хід роботи:**

1)Прочитали методичні вказівки до виконання лабораторної роботи

2)Написали програму для обчислення оберненого елемента за модулем з використанням розширеного алгоритму Евкліда

3) Знайшли 5 найчастіших біграм в своєму ШТ(1 варіант)

4) Написали програму для перебирання співставлення частих біграм мови та частих біграм ШТ, а також для обчислення а та б

5)Для кожного кандидата на ключ дешифруєм ШТ, перевіряючи його частоти букв, що повинні підходити середнім в мові

6) Розшифрували шифртекст за варіантом 1

**Результати**

Розшифрування тексту за варіантом 1:

Використавши основи модулярної арифметики, критерій відбору ключів та частотний аналіз, було знайдено таку пару ключів: a=654; b=777

Біграми шт ('вн', 56), ('тн', 51), ('дк', 50), ('ун', 50), ('хщ', 48)

Біграми рос. мови: СТ, НО, ТО, НА, ЕН

Зашифрований текст

*Вариант 1*

кеюибщаефдфмдкдкролрццисвнуншвйняэшскевдтнюдаобсюсыэихзтмдьлыохунхмьввнсдуэммндтихкеюибщыцязкзхшвносыотнйьщтцншуссянхщлвжвпькшвнмщзфтсхщпддкясввццтнавпьгнуьввйнлхиьерддыцрихэкьзцэижцьехщмсэкжлрибуждэмхимьпьявсттнзцюсфспьузйпдкнхркхульацкчашяьнсибжяксэкццзтчщиюцншумщошяьщкщнфрхуюижсгцыззфрщихзтчщрихнэпозтгфккчщкдмклыоьеынунййлцяьэрхнмкпмдкйыпоиэуныэнсмнмсхэццьедктництндуццоэивупхюфйчсьивйэютнрцшэбвщншуоздкдктнунянккфкяящиссбинкурдцбщшдскрщянщкдкяяищжшсвыьербщяяшндузйнкщнвнгоьцэииспьтуумщщшдекхндуаошдвдеигебуявюсшьйдроццвнфиибжлакццввбвываккчслтьхщзйьцжьбрьецфтспьбишиыовдьезбтнмсэкжллрчсхщьрпьшвшнйьяьнсибжлтьчсйьрьэчтнундулфтснсшбйнбжжцрнмющьккюиеуяэзтьяяреурндуьцоэгкмбобмщкскехюксдцтсывзтмсунйьксщиссшнчщзйьцйнпршьккфкяслркейьйнавпьхсуншнузеумкжлаклцисуьдьбкфипьйнмсуншснхтуйнццмсяьмныонкцркчыоклзфкчпьвныуозрбжлжвцнхщсссцжьбипсрзфкаьихмнщэчсавозулбутнзцнулцзткоццвнфиибхюпвиэислбиювинхыршьивцнярбщфджлзйьцйнзцнулцяьйнвнцхркпрыожврщьянкиюдждкеспьибубиюхщбуакикяеэдакаоццсвлбеилрлвцофкяяышвнунхщлвэкжлтьосцнхщиютнуншнмстспьлйаихщрнньнхшвщшвносчсабьешижсоэосыумщмбриввудябакфурщяэлчяздкаиьечслсосэкццяьцнэлязаьцнхщсссцжььзжлмщунавшьавзтьяюсуйвнакдуюиььяучмпрфдййвдихрнфззфтнхщхиеуяэзтьяыуццыьбьеелфеипвидийдкяязщпупзобчсуьвнлвмьтнчщьеэдвнстйндуаомнщоццвнфиибхюихтоццсввныклрынпьювюсисцйвнихчщлракющчьцнхщбщщйтннсхщдкищьешичщкздукчввзтьяакккйдищжлывьктзихывуллвовявшньсйссцпрыоынчкццяьклхнщэюдриисэкжллреуньыктзшрэчшиязиебчлвацлотнуншнмстспьицшэмвшщкзлоябсчбщшдыцэикзясусйнюйозвьтныэакосжцшншвюийдьяшншвосюсчязиьсунуллвихывхдскклмщубшскуаохщрнрцязакубсчфкяяосгйрщтнгбфдзйьцэибусчжвавмнззфдыоиюшсосюдритьйьнсхщтньцмнрнннстрсосуллвзтвднкцьяубщхичщмщтсчтгнэкхуямйдчщццмнрншвйнввлвацшвьхаврщшнищюиьсщожсюдгнуцрнчзшрынулцхдвмьцнрнуьнцяедьхсцнфуэюосйсчцэидктнуншнмншспьчшвнюдцфвдыоияосунйпщнбкчзиввнмнрьнсибчзлориисэибудкяспнззжлфсчсбкаышнтныьзтпэпьмвзтьсйядуццщщцспрчсэьлвзтклбулцшвюибщыцвивнуйвнакеичмывпвыэдчфкклццсвынуняуумпьшвшрцциссцмючщиюлврлиэйбдцриьцяьввюдаолыфьмодкчьяуфкойнкйдлцыцтнавчзфдыожяшсввдуюизбывщшвныэльидыщубшврчязрщвдойвнвнмщнсунцомюхщньюссттнхщщщфддбтьпнзкьеэдхнщьжвзтфрлцдкяяхьовюсстхщрнпьйнщофкпрынсиулйдццхифсчсхдййрснсерццисшнюсшьсцклтьпвидрошифкяяшнюдаоосунчзфпьцэилцмяэьсцклжшвнунакубакюйтносшнпьявывйнщожсунюэсцэиринкгеэдвэцнпдрщрнчстнввшвпвпьызмбйнвнцхпнуцязьсйядуулрибувдвнщозьгйбчйдсчбщиэбкдктнхщхилвннюсвнщокнирэчрниянцяеьцтсывзтосибфддбпмьлриввеэяьхэфртгрулцузбщшьавтулцибсчннисозфдыожллрдцбщшдскрщиэбквэгвжвзтшвжьаоеитншнпвихэхаорщибясфсчсщьавпьскггыоющлхвииспьвиулбутнзцнулцяьжцюсчвввйимюгвшнщиющюирсунлсгоьрыноьхоццвнфиибкзенуьпьбцрныгщйеуйнзщшьявхщеуеидебупьесузющдкясюэсцэиьцзттнмслдроавежбщяйрщйуюйлцеищьккффдкфьнхчщмщявисчтжьамаофисрябсчшижслбубщэнщфдэмсщябубчзйсанэирщхщмсэктзлэусхщрнляпдгсгцшфдкфьввнкубубяслоюищщшдекщсхдскхсовпннчубакакхуямдкяяхсвнхбжсмкщнщьжвэкссщьккдктнфифсбвбддкястнтнмслдьшсвьцйьшнсиеуюкыщцспрыьлнфкйдщщзйьцйныэвнхбрифкйыунрншьвнбкубьебчсвйнжндуеисхавупмююсшодкльулбусчцнннстрсшншвьхаврщянсцознкссьеуснсмнмснсибссвддцйнчсщнэпозцфибссщщубссвнхбрифкясхщфдцяьклрыоибсчфкщйвносэиэчпнзкццяьклакаолржцяьзтхдицфптнхщыглозфьцэидктнунэибунсхщавьвлващеутнищлрдцбщшдыцйнвнцхдздкицмяьхавьщвуцфьцжьщнмкпмдкяярнэирщввпноулцфрынщхыщмснфжврйвньркзскыщссвнхбрифкясозййцфцнюириьсосйгыовдриклакязеудкяяосузмщчявввнищрилвацшвьичдрщдкикгбмщбущстссвйьшвоейулцгйщщфкнхдкбщщйвнихобсчшибщекбщэюнхзциссичщиютнмслдфишдмбццмсгцшвэрзфвджяжвявшнмсчярщхьовюстымщкзищссыршьудццрреулфщщаефдхссироювяьисшщкзпксчролвтнрицнмскмжяявзтсиюгщхтнмспбмщбущськмюннисдкдкцфжвйьдтмщшвпвкмжяьямщшвжьрефщакиеэдакролфбклцбуябзщбукзунгэщьккгнввшнивжврщрныуоззнбкжлтьбцрныгйснжшдекцгеэюсрсхщньбиулбунхнчйдпнввкцйнуншвэьтнщоьцчсуьсцтгуьйнньосфипьявпьпршьйнлхавьщсиеуобмбмщбущсфрмщчяовупмюосшнкуаохщмсэкццзтбьыьмнжннуыфрыэиьсфсчсщьавозщсосгйлцмктзулынйнуйаихщавиэжьчщоуобмблвыьрнунокпмшрдцбщшддбубихйсансцрбжлвэкхюдрошджсюсунынмсйкмбкзхщхурсунщхввввмдкорыуснчзьяуиюшсвпнкурмщеувирсунсццьблшэннбвамозмщбвскаьшнжьжвупклэчйдищьешиивебпрябакоьзтянщиссйебчввтсзкиющьккбыоскчицпьявицчзивяьочлцсвпдгсуфдкфьяэюдаорибщвчрытнрсбидуаодункющхиьсхдгсунфрлцдкяяакдункчзжсюсбчкнбквьфзтнуноьюддкнхживналбуыодкеиочоьлхэфдкфьпьлннсвнмкхсмщтсывзтьятнакфкпрябйожсюсунюиикцфтсввщбакксйнбжрисцвджцмнщькмыгьяьехщсяюсстхщрнхщбщыцвиклаккзеущнюсияоусчтсйьзткллрццюсстшнюдкшвнгьерынньэьынавэкиютыннькиютноьакеишдщщшвпвмндтихжцшнйнюирсыэьяокпмаобщцсэщбушсхщмсэкссьейпфкясищхнэкмбжлжвннстрсосщэтсяьяубщыцввяфжсюсунтсчтгвмьввьелвмкрюеэзтдцццрнмюхщбуакдожсвнйсзвпьфихщчсяьзтьяйкчзфсчсгэлнцнерссжофкеиябпвистнпвюскиосырынщэгожсгцмефдфмжяосзкццзтпытнрсакьлмщриарзфеуэирибщхиьсуйвнихвнстйнянцуфкщщцсунхдицяедьакхуумжсвнчрлвньзтьяйкчзезьцюсжрыщумьцэиясезьцвнвнунищьеяцпьерынхщщщыцвиьянсибясшнлсиьпвтснфюирыюсцьаккнивжошижсмкарссжозщццесшндцнсккаирсыэокпмщнввйкриаршьлнуьэиулбунхмокздцрнфзфпдкяспнчкхуцфюижсшщязюсшсиэжьввшвяэосрнеелоюисьфиосэщублыунчяюэецчзивяьокхуямщщшдбофдгвмсжкддьяжьяущнввввшнмьвврщозенйсуньейпфкаьтныоеущькхзцнулцзтднчелвпьгцбуавкмлыклтьяуаишдщщмюкеоубщыцвиакэмлхчярщтсчтрьйнвнцхмьакггмщшджсунлххэхьзтлрэчбудкввзнввшнжьжврщунынжвжрццисчцэиаьмчвврщищссркжэжвмндтфрлцяьклхнгцязвэкьзцэиьшсвмдьцюяусиебчдуьешдриезмщюиоуриесввхьовэкжятнмслдзьлсрщйносыклрлврнввлэусхщрнавпьгбубсвйнавдьоспншсмкпрынкчмсхщнкойщщбщшдмефдфмжлрифсбвбддкяяыоввйнщцыгевввйьмэоьжйвнакеиэчпьидфккнйкрижэпншнхщынгспнунрнгошддкяяфсшьыоарфдрижлццэччсавпьзншвйнрнкизфтсиспьнкгбмщбущссцшнмьввьщянмсхмдктнянккбщшдекццжлывйквэпншнхщынгспныэрнгошддкйыявзтцнюфввовявлиьцяьокпмаишнмнээхфкччтхдицивьспьгсунмщпвюдцфюирыусунлрлцдкяяыуаокнввпьфзлцвнстбвхщщслэмдчзоулыфьтглозфьцэидкнхпрынкчмстспьвифщгбрыяьцщжлзфпреурндцвныкмбарбуябакфккчявпвлсзврщьяшнынйнмьунжкиюхщлвхщпэжвчспьпрццсвпддктндклцнулцмклытсющшдекццзтиэярчсжвюсстибдцньтсюсстхщээрщьечщкзмщрнтслкеурьйомюхщньюссттнулбуввзнтснфчзццзтвииярщьякбньависйщкзхщхуиюшннуяетнхщюиакфккчлспьыопьрцмнрншбынлсюдризьяуфкшдвчсксчавзтрщхсщв

Розшифрований текст

убиватыболышененадопослетогокаконужеубилноследуетецубьтыблхгшдарньйюначепришлосыбьубиватесамомуэтонешдноиюшыдоброесострадакюеэтоотождествлениенаосновакюиобюнаковьтюмпулесовкуююйствусдбственноговорялишывйюкюмалынойстепекюсмещенньйнаруюссизмэпюческаяценностыэтойдобротьэпюмнеоспариваетсйможетбьтыэтовообщемеханизмнашегшддбыогоучаспюяпоотношенликдругоцучеловекуосдбеннояснопроступающийвчреэвьчайномслучаеобремененногосознаниясвоейвиньписателянетсомнениячтоэташюмпатияпопричинеотождыствлекюярешителыноопределилавьборматенюаладостоевскогоносначахаонизэглюстичысзюхпдбуждекюйвьвшдилдбькновенногопрестйпкюкапоиюпюческоглюреиюаюозногопреждечемкконцусвоейгюзнивернутызякпервопрыступникукотцеубийцеисдехатывегоиюцесвоепоэтичыскоепнюзнаниеопубиюковакюеегопосмертногонаслебюьюдневкюковегоженьяркоосвепюлошдинэпизшдегожизкютомремякогдадостоевсзюйвгерманеюбьлобуреваемигорнойстрастыюдостоевскийзарулеткойявньупнюпадокпатологичыскойстраспюкоторьйнепшддаетзяинойоценкекюскакойстороньнебьлонедостаткавоправданияаэтогостранноглюнедостойногоповедекюячувствояюнькакэтонередкдбьваетунемротиковнашлоконкретнуюзаменувдбремененноспюдолгамеюдостоевсзюямоготгованюватызятемчтоонпривоюгрьшеполучилбьвозможностывернутызямросшюыюзбежавзаключениявтюрымукребюторайюноэтдбьлтолыкопредлогдостоевскийбьлдостатовнопыокюцателенчтобьэтопонятчюдостаточночестенчтдбьвэтомпризнатызяонзналчтогхачньмбьхаиграсамапозебевсепшдыобноспюегообусловленногоперяювньмипозьвамибезрассудногоповедекюяслужаттомудоказателествомиещекоечемрюноцуоннеуспокаивалзяпоканетерялвзегоиграбьхадлянеготакжесредствомсамонаказаниянесчетноеколичыствораздавалонмолшдойженесловлюиючестноысловоболышенеигратыилинвюгратывэтотденыионнарушалэтословокаконарасскаэьваетпочтивзегдаеслионсвоимипыоигрьшайюдовобюлсебьюеедокрайнебедственногоположекюяэтослужилшдлянегоещеоднимпатолоаюческимудовлетворениемонмогпередниипоношютыиукюжатызебяпроситыеепредюратыегораскаиватесявтомчтоонавьшхазацужзанегостаыогогрешкюкаипослевсейэтойразгрузкисовыспюнаследцицюйденчюграначиналасесноваимолшдаяженапривькхакэтоцууюклютаккакзаметилачтотоотчеговдейстяютелыноститолыклюможндбьлоогюдатыспасениямюсателыствокюкогданепыодвигалосывпередлучшечемпослепотенювсеглюзакладьванияпоследнегоимущыствасвядювсегоэтогоонаконечнонепокюмахакогдаегочувствовиньбьлоудовлетворенонаказакюймиккоторьмонсамзебяприговорилтогдэюсчезалазатрудненностывработетогдаонпозволялсебысдехатынесколыкошхговнапупюкуспехурассматнюваярассказболеемолшдогописателянетрудноугадатыказюедавнопозабьтьедетскиеперегювакюянахшдятвьявлекюявигорнойстраспюустефанацвейгапосвятившегомеждйпыофюмдостоевскомуобюкюзсвотхочерковтнюмастеравсборкюкесмятениечувствыстыновелладвадцатычетьречасавгюзниженцюньэтотмаленызюйшедеврпоказьваеткакбудтолишытокакимбезответственньмсуществомявляетсяженцюнаинакакиеудивителыньедлянеесамойзакононарушенияеетолкаетнеогюданноегюзненноевпечатлениеноновеллхэтаысиюподвергнютыеепшюхоаналитичыскоцутолкованлиговонютоднакдбезтакойоправдьвающейтенденуюигораздоболышепокаэьваетсовсеминоедбщечеловеческоеилискорееобщемужскоеитакоетолкованиестолыячнопшдсказаночтонетвозможноспюегонедопуспютыдлясущносттхудожыственноготворчестваларактерночтописателескоторьмменясвяэьваутдружысзюеотношениявответнамоирасспыосьютверждалчтойпомянютоетолкованиеемучуждоивовзеневхшдиловегонамерениянесмотрянаточтоврасскаэвплетеньнекоторьедетаиюкакбьрассчитанньенаточтобьуказьватынатайньйследвэтойновеллевеликосветскаяпожилаядамаповеряетмюсатеоиотомчтоеупнюшлосыпережитыболеедвадцапюлеттомуназадраноовдовевшаяматыдвухсьновейкоторьечнейболеененуждаиюсыотказавшаязяотказюхбьтонибьлонадежднасороквторомгодугюзнионапопадаетвомремяодноглюзсвотхбесцелыньхпутешестяюйвигорньйзалмонакскогокадюногдысребювсехбюкояюнеевкюмакюепнюковьваутдверукикоторьеспотрясающейнепосредственностыыюшюлойотркжгитвзеперегюваемьенесчастньмигыокомчувстварузюэтирукикрашювогоюношиписателыкакбьбезовсякогоумьсладелаетегоыовесникомстаршегосьнанаблюдгищейзэюгройженщиньпотерявшеговсвювглубочайшемотчаянеюпозюдающегозалчтдбьвпаркепоконфютысосвоеюбезнадежнойгюзнюинеизяскюмаясимпапюязаставляетженцюнуследоватызгиношейвпредпринятывзедляегоспасенияонпринимаетеезаоднрюзмногофюсленньхвтомгоршденавязфювьхженцюкюхочетотнееотдехатызяноонанепокидаетегоивьнужденавконцеконцоввсилуслогювштхзядбстоятелыствостатесявегономереотеляираздеиютыегопостелыпослеэтожюмпыояюдюыованнойоибочнойнофюонавелитказалосыбьуспокоившецузяюношедатыейторжественноедбещаниечтоонникогдаболышенебудепюгратеснабжаетегоденыгайюнадбратньйпутыисосвоейстороньдаетобещакюевстрепютызяснимпередуходомпоезданавокзаленозатемвнеупыобуждаетсяболышаянежностыниношеонхготовапожертвоватывземчтобьтолыкосохранитыегодлясебьюонарешаетотпраяютызяснимвмыстевпютешыствиевмыстотогочтдбьскюмпыоститесявзяческиепометюзадерживгитевюонаопаздьваетнапоездвтоскепоисчезнувшецуюношеонасновапнюхобютвигорньйдомисвозмущениемобнаруживаеттамтежерузюнакануневозбудивхюевнейтакцигорячуюсимпапююнарушителыдолгавернулзязюгреонанапойюнаетемуобегодбещанеюношдергюмьйстрастыюонбракютсорвавшциеглюгрувелитейубиратесявонишвьряетденыаюкоторьйюонахотелаеговькумютыопозореннаяонапозюдаетгоыодавпоследствеюузнаетчтоейнеудалосыспаспюегоотсамоуююйствхэтаблыстящеибезпрдбеловвмотивировкенамюсаннаяновеллэюмеетконевноправонасуществовакюекактаковаьюнеможетнепыоизвестиначитателяболышоговпечатленияшднакопстхоанаиюзуфютчтоонавозкюкланаосновеумопостыояемоговожделенияпенюшдаполовогосозревакюяокаковомвожделекюинекоторьевспойюнаутсовершенносознателыносогхасноумопостыояемоцувожделенлиматыдолжнасамаввыспююношувполовуюжизныдляспазекюяегоотзаслуживгищегоопасениямредаонакюзмастолычастьесублимирцицюехудожыственньепыоизведекюявьтекгипюзтогожепервоистовникапороконанизмазамещаетзяпоыокойюгорнойстрастиударекюепоставленноенастрастнцидеятелыностырукпредателыскисяюдетелыствуетдбэтомотводеэнераюидейстяютелыноигорнаяодержимостыявляетзяэкяювалентомстаройпотребностивонанизмекюшдкюмсловомкыомесловэюгранелызяназватыетееаа-